DETAILED ACTION

Acknowledgements

1. This communication is in response to the amended Application No. 10/764,345 filed on 10 March 2010.

2. Claims 1, 4-6, 9, 13, 16-23, 24, 24-25 are currently pending and have been fully examined.

3. For the purpose of applying the prior art, PreGrant Publications will be referred to using a four digit number within square brackets, e.g. [0001].

Response to Applicant's Remarks/Amendments

4. Applicant's response, filed on 10 March 2010, have been fully considered, but are not persuasive. Examiner would like to point out that Applicant's newly added language, and in other limitations, of "weights associated with the rational statistics of the one or more regions are pseudo-randomly generated based at least upon different secret keys, one different secret key for each region of the one or more regions,…" is descriptive in nature and not a positive recitation of a method step.

Clauses (e.g. whereby, thereby, wherein) that merely states the result of the limitation(s) of a claim(s) does not limit the scope of the claim(s).[1] Therefore, as in claim 1, and others, what the rational statistics represent for example, will not limit the scope of the claim.

Claims 4-6, 9, 13, 18 contains similar language found in claim 1.

In light of Applicants' choice to pursue method claims, Applicants are also reminded that functional recitations using the word "for," "configured to," or other functional terms (e.g. see claim 13, which recites, “partitioner configured to…calculator configured to…quantizer configured to…etc.) have been considered but are not given patentable weight[1] because they fail to add any structural limitations and are thereby regarded as intended use language. To be especially clear, all limitations have been considered; however a recitation of the intended use in a method claim must result in a structural difference between the claimed product and the prior art in order to patentably distinguish the claimed product from the prior art. If the prior art structure is capable of performing the intended use, then it reads on the claimed limitation.[2] Unless expressly noted otherwise by the Examiner, the claim interpretation principles in this paragraph apply to all examined claims currently pending.

Therefore, after careful review of Applicant’s points of contentions, the Examiner respectfully disagrees with the Applicant and maintains his rejection.

[1] In re Gulack, 703 F. 2d 1381, 217 USPQ 401, 404 (Fed. Cir. 1983)(stating that although all limitations must be considered, not all limitations are entitled to patentable weight);

[2] In re Casey, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) ("The manner or method in which such machine is to be utilized is not germane to the issue of patentability of the machine itself."); In re Otto, 136 USPQ 458, 459 (CCPA 1963). See also MPEP §§ 2114 and 2115.

Claim Objections

5. The numbering of claims is not in accordance with 37 CFR §1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Miss-numbered claims 24 24 25 it is unclear how the Applicant desires to have his claims numbered.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. §101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 13, 16-17, 23, 24, 24-25 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Claim 13 is directed to a system comprising:

> a partitioner configured to segment a digital good into a plurality of regions;
>
> a region-statistics calculator configured to:
>
> calculate statistics of one or more of the plurality of regions, wherein the statistics of the one or more of the plurality of regions are representative of respective one or more of the plurality of regions,
>
> generate the statistics of the one or more of the plurality of regions via a hashing function having a quotient of two weighted, linear, statistical combinations, wherein weights associated with each region of the one or more of the plurality of regions are correlated with one another within each region;
>
> a region quantizer configured to quantize the rational statistics of the one or more of the plurality of regions; and

> a digital-goods marker configured to generate a marked good using the quantized rational statistics.

Even though the claim recites “system” the body of the claim discusses “calculator” and it does not recite any actual technical system **components**. A system or apparatus claim should always contain the **structure** or the **hardware** that performs the function Applicant claims. Applicant’s Specification recites:

> [0087] FIG. 6 shows a methodological implementation using the digital-goods hashing function (depicted above in Equation 1). **This methodological implementation may be performed in software,** hardware, or a combination thereof. For ease of understanding, the method steps are delineated as separate steps; however, these separately delineated steps should not be construed as necessarily order dependent in their performance.

Therefore, the claimed method is non-statutory and therefore rejected under 35 U.S.S. §101.[1]

Claims 16-17, 23, 24, 24 and 25 are also rejected for being dependent upon rejected claim 13.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. §112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 1 and 4-6 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As to claim 1, Applicant recites, “one different “**secret key**” for each region of the one or more regions;” however, this limitation makes it appears that there is an "association" between a "secret key" and a particular region. However, Applicant's Specification does not teach this “association.” Applicant Specification recites:

> [0092] At 616: For each chosen region R.sub.i, the exemplary watermarker uses the cryptographic key k to generate a set of weights [a.sub.ij] for each coefficient s.sub.j.di-elect cons.R.sub.i. (a.sub.ij=0 otherwise.) The weights are generated independently for different regions, overlapping or not.

Applicant’s section [0092] does not adequately teach an association. Additionally, Examiner would argue there is a distinction between a “secret key” used in Applicant’s claim limitation and a “cryptographic key” taught in Applicant’s Specification. Applicant’s Specification teaches the use of a “cryptographic key” for each region, not a “secret key.” Applicant’s Specification recites a distinction between a “secret key" and a “cryptographic key.”

Claims 4-6 are also rejected for being dependent upon rejected claim 1.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. §112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 1, 4-6 and 19-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 is rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: associating weights with rational statistics…acquiring/receiving different secret keys. It is unclear where or how these "secret keys" are derived or acquired from. One of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim 18 contains similar language or like deficiencies found in claim 1.

Claims 4-6 and 19-22 are also rejected for being dependent upon rejected claim 1.

Claim 9 is rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: instructions to perform the function of mapping…instructions for dimensionality reduction. It is unclear how these limitations are being performed without first establishing them. One of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

The term "**ideal** low-pass filter" in claim 18 is a relative term which renders the claim indefinite. The term "**ideal**" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim 20 contains the same language or like deficiencies found in claim 18.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. §103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1, 4-6, 9, 13-24, 24 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Venkatesan et al., (US 2004/0001605) ("*Vankatesan*").

As to claim 1:

Venkatesan teaches substantially as claimed:

> obtaining a digital good ([0085]-[0093], Claim 1);
>
> partitioning the digital good into a plurality of regions ([0085]-[0093], Claim 1);
>
> calculating rational statistics of one or more regions of the plurality of regions,
>
> wherein ([0085]-[0093], Claim 1):
>
> the rational statistics of the one or more regions are representative of respective one or more regions,
>
> the rational statistics of the one or more regions are generated via a hashing function having a quotient of two weighted, linear, statistical combinations ([0085]-[0093], Claim 1);
>
> the rational statistics are semi-global characteristics ([0085]-[0093], Claim 1):
>
> quantizing the rational statistics ([0085]-[0093], Claim 1);
>
> marking the digital good with the quantized rational statistics of the one or more regions of the plurality of the regions ([0085]-[0093], Claim 1);
>
> one different secret key for each region of the one or more regions ([0051], [0092], [0206]);

Vankatesan does not expressly teach:

> weights associated with the rational statistics of the one or more regions are pseudo-randomly generated based at least upon different secret keys;

However, Official Notice is taken that using a secret key to use a pseudo-randomly generated weight is old and well known in the related art. For example, in the related art, employing the use of secret key in the generation of randomly generated weights aids in its security. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Vankatesan with the commonly recognized practice of weights associated with the rational statistics of the one or more regions are pseudo-randomly generated based at least upon different secret keys.

As to claims 4 and 17:

Venkatesan expressly teaches:

wherein the hashing function is represented by ([0131]-[0144]);

$$h_i = \frac{\sum_{j \in R_i} \alpha_{ij} s_j}{\sum_{j \in R_i} b_{ij} s_j}$$

Where:

- a_{ij} is the j^{th} element of a_i and a_i are a pseudo-random generated weight factors;
- b_{ij} is the j^{th} element of b_i and b_i are a pseudo-random generated weight factors;
- s denotes the digital good of dimension N × 1;
- R_i are the plurality of regions, where $R_i \subseteq \{1,2,\ldots,N\}$.

<u>As to claim 5:</u>

<u>Venkatesan</u> expressly teaches:

> wherein the partitioning comprises segmenting the digital good into a plurality of overlapped regions ([0092], Claim 2);

<u>As to claim 6:</u>

<u>Venkatesan</u> expressly teaches:

> wherein the marking comprises embedding a watermark via quantization ([0100], [0106], Claim 8);

<u>As to claim 9:</u>

<u>Venkatesan</u> teaches substantially as claimed:

> obtaining a digital good ([0085]-[0093], Claim 1); and
>
> using quantization, marking the digital good with a watermark, wherein ([0085]-[0093], Claim 1);
>
> the quantization is based upon semi-global characteristics of regions of the digital good ([0085]-[0093], Claim 1);
>
> the semi-global characteristics are generated via a hashing function employing a quotient of at least two weighted linear combinations of statistics of the regions of the digital good ([0085]-[0093], Claim 1);
>
> wherein a change in a hash vector space of the hashing function is mapped to a data space of the digital good and a dimensionality reduction from the data space of the digital space to the hash vector space of the hashing function occurs ([0085]-[0093], Claim 1);

<u>As to claim 13:</u>

<u>Venkatesan</u> teaches substantially as claimed:

> a partitioner configured to segment a digital good into a plurality of regions ([0085]-[0093], Claim 1);

> a region-statistics calculator configured to ([0085]-[0093], Claim 1);
>
> calculate statistics of one or more of the plurality of regions, wherein the statistics of the one or more of the plurality of regions are representative of respective one or more of the plurality of regions ([0085]-[0093], Claim 1);
>
> generate the statistics of the one or more of the plurality of regions via a hashing function having a quotient of two weighted, linear, statistical combinations, wherein weights associated with each region of the one or more of the plurality of regions are correlated with one another within each region ([0085]-[0093], Claim 1);
>
> a region quantizer configured to quantize the rational statistics of the one or more of the plurality of regions ([0085]-[0093], Claim 1); and
>
> a digital-goods marker configured to generate a marked good using the quantized rational statistics ([0085]-[0093], Claim 1);

<u>As to claim 16:</u>

<u>*Venkatesan*</u> expressly teaches:

> wherein the partitioner is further configured to segment the digital good into a plurality of overlapping regions ([0030], [0044], [0065], [0073], [0088], Claim 42, Figure 3);

<u>As to claim 18:</u>

<u>*Venkatesan*</u> teaches substantially as claimed:

> obtaining a digital good ([0085]-[0093], Claim 1);
>
> partitioning the digital good into a plurality of regions ([0085]-[0093], Claim 1);
>
> calculating rational statistics of one or more regions of the plurality of regions ([0085]-[0093], Claim 1);
>
> wherein:
>
> the rational statistics of the one or more regions are representative of respective one or more regions ([0085]-[0093], Claim 1);

> the rational statistics are semi-global characteristics ([0085]-[0093], Claim 1);
>
> the rational statistics of the one or more regions are based upon a quotient of two weighted, linear, statistical combinations ([0085]-[0093], Claim 1); and
>
> the calculating further comprises:
>
> independently generating pseudo-random weights for the one or more regions based at least upon different secret keys, one different secret key for each of the one or more regions ([0085]-[0093], Claim 1); and
>
> generating weights that are correlated with one another within each of the one or more regions by passing respective pseudo-random weights for each of the one or more regions through an ideal low-pass filter ([0085]-[0093], Claim 1);
>
> quantizing the rational statistics ([0085]-[0093], Claim 1);
>
> marking the digital good with the quantized rational statistics of the plurality of the regions, wherein the marking comprises embedding a watermark via quantization ([0085]-[0093], Claim 1); and
>
> wherein a cutoff frequency of the ideal low-pass filter controls a tradeoff between security and robustness of the watermark, and affects a distortion level of the marked good both in a mean-square-error (MSE) sense and in a perceptual sense ([0085]-[0093], Claim 1);

As to claim 19:

Venkatesan expressly teaches:

> wherein the calculating further comprises generating correlated weights from the pseudo-randomly generated weights for each of the one or more regions, the correlated weights being correlated with one another within each of the one or more regions ([0085]-[0093], Claim 1);

As to claim 20:

Venkatesan expressly teaches:

> wherein the generating comprises passing the pseudo-randomly generated weights for each of the one or more regions to an ideal low-pass filter to generate the correlated weights ([0085]-[0093], Claim 1);

<u>As to claim 21:</u>

<u>*Venkatesan*</u> expressly teaches:

> wherein the marking comprises embedding a watermark via quantization, and a cutoff frequency of the ideal low-pass filter controls a tradeoff between security and robustness of the watermark ([0085]-[0093], Claim 1);

<u>As to claim 22:</u>

<u>*Venkatesan*</u> expressly teaches:

> wherein a cutoff frequency of the ideal low-pass filter affects a distortion level of the marked good both in a mean-square- error (MSE) sense and in a perceptual sense ([0085]-[0093], Claim 1);

<u>As to claim 23:</u>

<u>*Venkatesan*</u> expressly teaches:

> wherein the region-statistics calculator is further configured to generate pseudo-random weights for each region of the one or more regions, and the correlated weights associated with each region of the one or more regions are generated by passing respective pseudo-random weights generated for each region to an ideal low-pass filter ([0085]-[0093], Claim 1);

<u>As to claim 24:</u>

<u>*Venkatesan*</u> expressly teaches:

> wherein the digital-goods marker is further configured to embed a watermark onto the digital goods to form the marked good, and a cutoff frequency of the ideal low-pass filter controls a tradeoff between security and robustness of the watermark ([0085]-[0093], Claim 1);

<u>As to claim 24:</u>

<u>*Venkatesan*</u> expressly teaches:

> wherein a cutoff frequency of the ideal low-pass filter affects a distortion level of the marked good both in a mean-square-error (MSE) sense and in a perceptual sense ([0085]-[0093], Claim 1);

As to claim 25:

Venkatesan expressly teaches:

> wherein the pseudo-random weights for each region of the one or more regions are generated based at least upon different secret keys, one different secret key for each region ([0085]-[0093], Claim 1);

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- *Obana* (US 2001/0016911); [0011] In accordance with a first aspect of the present invention, there is provided a signature calculation system by use of a mobile agent, comprising: a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent from which the mobile agent starts moving in a network; and remote hosts in the network which can be visited by the mobile agent. The base host includes an agent execution environment, a random number generation means, a partial signature auxiliary data generation means and a public key cryptography calculation means. The agent execution environment lets the mobile agent execute its program code. The random number generation means generates random numbers. **To the partial signature auxiliary data generation means, the random numbers generated by the random number generation means and a secret key of the owner of the mobile agent are inputted.** The partial signature auxiliary data generation means generates partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to the remote hosts so that the partial signature auxiliary data will be used when partial signatures necessary for the calculation of the digital signature of the owner of the mobile agent are calculated by remote hosts. The public key cryptography calculation means conducts encryption and signature calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means. Each remote host includes an agent execution environment, a partial signature calculation means, a partial signature combining means and a public key cryptography calculation means. The agent execution environment lets the mobile agent execute its program code. To the partial signature calculation means, signature target data, data which have been carried by the mobile agent, and a secret key of the remote host are inputted. The partial signature calculation means calculates a partial signature which is necessary for the calculation of the digital signature of the owner of the mobile agent. To the partial signature combining means, one or more partial signatures calculated by one or more remote hosts are inputted. The partial signature combining means outputs the digital signature calculated for the signature target data by use of the secret key of the owner of the mobile agent. The public key cryptography calculation means conducts encryption and signature calculation for the partial signature calculated by the partial signature calculation means. The mobile agent, which started from the base host carrying the partial signature auxiliary data and which is arbitrarily presented with the signature target data by a remote host, stores the signature target data if the mobile agent determined to write the digital signature for the signature target data by use of the secret key of the owner of the mobile agent, and thereafter visits k (k: security parameter) remote hosts and carries the partial signatures calculated by the remote hosts to the remote host that presented the signature target data. At the remote host that presented the signature target data, the digital signature for the signature target data by use of the secret key of the owner of the mobile agent is obtained from the partial signatures calculated by the k remote hosts.

Any inquiry concerning this communication or earlier communication from the examiner should be directed to Mr. Dante Ravetti whose telephone number is (571) 270-3609. The examiner can normally be reached on Monday – Thursday 9:00am-5:00pm.

If attempts to reach examiner by telephone are unsuccessful, the examiner's supervisor, Mr. Calvin Hewitt may be reached at (571) 272-6709. The fax phone number for the organization where this application or proceeding is assigned is (571) 270-4609.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system see http://pair-direct,uspto.gov. Should you have questions on access to the private PAIR system, please contact the Electronic Business Center (EBC) at 1-(866) 217-9197. If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 1-(800) 786-9199 (IN USA or CANADA) or 1-(571) 272-1000.

/Dante Ravetti/
Examiner, Art Unit 3685
Tuesday, June 01, 2010

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685